Council of the European Union

Brussels, 19 June 2025
(OR. en)

10269/25

LIMITE

PROCIV 72

'I' ITEM NOTE

From:	Presidency
To:	Permanent Representatives Committee (Part 2)
Subject:	Report from the Polish Presidency on the main achievements at EU level in the field of critical entities resilience

Delegations will find in annex the Report from the Polish Presidency on the main achievements at EU level in the field of critical entities resilience.

COREPER is invited to take note of the report.

Report from the Polish Presidency on the main achievements at EU level in the field of critical entities resilience

This report outlines the principal achievements, developments and strategic directions taken during the Polish Presidency of the Council of the European Union in the field of critical entities resilience, covering the period from January to June 2025. Over the course of its term, the Presidency convened four formal meetings of the PROCIV-CER Working Party—on 5 February, 18 March, 14 April, 13 May and 24 June —as well as co-organised an international conference in Warsaw (1–2 April) on the methodology for assessing the risks of disruption of essential services. These sessions enabled structured dialogue between Member States, the Commission, EEAS, and relevant stakeholders, focusing on various measures to enhance infrastructure resilience across the UE.

1. Presidency Priorities

At the beginning of its term, the Polish Presidency set out four thematic priorities to guide its work in the PROCIV-CER Working Party. These included the advancement of standardisation practices in the field of critical infrastructure resilience, the refinement of national and EU-level risk assessment methodologies, and a focused response to the growing threat of hybrid attacks. These themes reflected both the evolving risk landscape and the need to strengthen coherence in policy and practice across Member States.

With regard to standardisation, the Presidency facilitated a structured exchange on the use and role of standards, covering both non-binding international and binding and non-binding national ones. This dialogue was grounded in a questionnaire circulated among Member States, the results of which were discussed during dedicated sessions of the Working Party.

In addressing the issue of risk assessment, the Polish Presidency placed strong emphasis on encouraging dialogue and mutual exchanging views, rather than prescribing fixed solutions. This approach culminated in the organisation of an international conference in Warsaw, co-hosted with the European Commission (DG HOME), which brought together Member States, EU agencies, academics, and critical infrastructure (CI) operators. Experts exchanged views on national methodologies, discussed areas of possible convergence, and considered the added value of integrating civil protection, cybersecurity and CER (Critical Entities Resilience) risk perspectives. The Presidency also presented a national framework as a practical example, illustrating how risk mapping can take into account sectoral interdependencies and evolving threat scenarios. Discussions highlighted the importance of clarity, flexibility, and scientific rigour in designing effective risk assessment models.

Hybrid threats were identified by the Polish Presidency as a cross-cutting and increasingly relevant dimension of critical infrastructure resilience. In light of recent incidents affecting energy, transport, and digital networks, the Presidency underlined the need to consider hybrid threats as factors that can significantly disrupt essential services. An in-depth discussion on this matter in the Working Party is planned for end of June and, in addition, the topic has already been reflected in broader exchanges, particularly in relation to undersea cable security and risk assessment. In addition to the planned June discussion, the Presidency will deliver a dedicated presentation focused specifically on hybrid threats to critical infrastructure. To support this work, the Presidency has collaborated with a governmental publishing house on drafting a special issue of the academic publication "Terrorism. Studies–Analysis–Prevention", entitled "Terrorist and Sabotage Threats to Critical Infrastructure", dedicated to current challenges and practical considerations related to hybrid threat preparedness in the CER context. The issue will be presented in June. The Presidency maintained close cooperation with the Horizontal Working Party on Enhancing Resilience and Countering Hybrid Threats (HWP ERCHT).

2. Enhancing Resilience and Risk Awareness

The Polish Presidency placed strong emphasis on cross-sectoral interdependencies and vulnerabilities in supply chains as key components of infrastructure resilience. During the March meeting of the PROCIV-CER Working Party, some Member States showcased concrete models for sectoral coordination and risk mitigation.

A further step was taken during the abovementioned international conference in Warsaw (1-2 April), where these issues were explored in greater depth. Session 2 of the event focused on scenario-based planning and forecasting tools. Experts presented practical approaches for vulnerability analysis and supply chain stress testing, highlighting the importance of flexible models that can account for cross-sectoral complexity. Session 3 addressed integrated supply chain resilience, with particular emphasis on managing external dependencies and enhancing cross-border coordination.

These discussions helped identify common challenges as well as areas for joint action. The Presidency considers the exchange a strong foundation for future work and encourages the incoming Presidency to continue exploring this topic. The analytical groundwork established—including detailed national insights and examples—offers a solid basis for informed policy development.

3. Standardisation

Throughout the semester, the Presidency facilitated discussions on the relevance of standards in supporting the development of national policies on critical infrastructure resilience as well as the

implementation of the CER Directive. Member States debated the applicability of international frameworks and the need for sector-specific adaptations.

A key element of this exchange was the presentation of Poland's own non-binding standards, shared as an example of good practice and a tool for building common understanding. Additionally, a technical presentation delivered during the February meeting by representatives of the Confederation of European Security Services (CoESS) offered further analytical insights to support the discussion.

The Presidency placed particular emphasis on fostering a structured exchange of views—initiated through a questionnaire—and creating space for comparing approaches in an open and constructive setting. The discussions helped identify key policy and operational questions that could usefully be explored further in future work. As such, the topic remains open for deeper consideration under the incoming Presidency, with a strong substantive basis already established. A detailed summary of Member State responses to the questionnaire is compiled in a separate Presidency report.

4. Cable Security and Cross-sector Coordination

The publication of the *EU Action Plan on Submarine Cable Security* on 21 February 2025 marked a key turning point during the Polish Presidency. The PROCIV-CER Working Party was designated as the lead group responsible for its follow-up, making cable security a central theme of the March, April, and May meetings.

In March, the Commission and EEAS presented an overview of the Action Plan, followed by an initial exchange of views with Member States on strategic vulnerabilities and coordination needs. The April meeting focused more specifically on threat detection and monitoring capacity, with the Presidency providing an update on the state of play and inviting technical reflections from delegations.

The May meeting deepened this discussion with a series of thematic presentations. These included:

- an overview of International Telecommunication Union (ITU) activities related to the protection of telecommunication underwater cables;
- a briefing on the Integrated Maritime Services for maritime surveillance in support of Member States;
- updates from the Commission on the work of the Submarine Cable Infrastructure Expert Group;

- and a detailed session on improving underwater cable repair capabilities, featuring both a Commission presentation and a national case study from Finland on deployable modular solutions.

Throughout this period, the Presidency also conducted a written consultation, gathering responses from 14 Member States on national frameworks, detection capacities and interagency coordination. The results of this consultation were compiled and analysed in a detailed Presidency report, which served as a reference point for further discussions within the Working Party and may provide a useful basis for continued work under the incoming Presidency.

5. Risk Assessment Methodologies

A central thematic focus of the Polish Presidency was the advancement of analytical tools and methodologies for assessing risks to essential services. To this end, the Presidency co-organised with the European Commission (DG HOME) an international conference in Warsaw entitled *Methodology for Assessing the Risk of Disruption of Essential Services*, which provided a comprehensive overview of current research, national practices, and emerging threat models.

Discussions opened with reflections on institutional preparedness and the importance of maintaining public trust during crisis situations, with emphasis placed on the role of digitalisation and data-informed governance. In the business continuity session, representatives from the energy sector shared detailed case studies, including a risk assessment model for the Polish LNG Terminal based on 420 custom-built attack scenarios covering land, maritime and aerial vectors. The methodology relied on threat feasibility and attacker capabilities rather than fixed probability scores.

Academic contributors introduced structured, index-based approaches to risk quantification. One model combined hazard probability, impact categories, and an aggregated risk index, with dynamic adaptation mechanisms for national authorities. Other speakers underscored the value of scenario planning and qualitative threat mapping in areas where quantitative data remain limited.

A full session was dedicated to emerging and hybrid risks, with insights from the OECD, JRC, and national research institutes. Topics included global cascading threats (e.g., geomagnetic storms, space debris), conceptual governance models such as JRC's CORE framework, and systemic vulnerabilities linked to artificial intelligence. AI-related threats—such as data poisoning, adversarial manipulation, and autonomous malware—were identified as critical areas requiring regulatory scrutiny, technical resilience, and public-private coordination.

The second day of the conference addressed the resilience of supply chains and essential services under conditions of geopolitical stress and military threat. EU-level monitoring frameworks, including the JRC's real-time analytics under the Chips Act, were presented alongside national case studies on trade dependencies and transport vulnerabilities. Examples from Poland and Finland illustrated how geopolitical factors can directly impact the resilience of critical infrastructure.

A dedicated session on military resilience and service continuity drew operational lessons from the war in Ukraine, with detailed findings from national institutions on how to maintain essential functions during conflict. These included cloud migration under duress, whole-of-society defence concepts, and counter-disinformation strategies.

Taken together, the conference outputs offered a rich repository of methodological approaches, real-world testing, and forward-looking risk governance models.

6. Cooperation with Other Council Working Parties

Recognising the cross-sectoral nature of critical infrastructure resilience, the Polish Presidency consistently sought to coordinate its work within the PROCIV-CER Working Party with related policy discussions in other Council formations.

In February, the Presidency invited the Ad hoc Working Party on Preparedness, Response Capability and Resilience to Future Crises to present reflections from the report *Safer Together – Strengthening Europe's Civilian and Military Preparedness and Readiness*. The exchange served as a basis for aligning broader preparedness agendas with the operational goals of the CER Directive.

In March, the tabling by the Commission of the *EU Action Plan on Submarine Cable Security* called for effective cross-Working Party cooperation in the Council. Delegates from the Working Party on Telecommunications and Information Society, PROCIV, the Horizontal Working Party on Enhancing Resilience and Countering Hybrid Threats, the Horizontal Working Party on Cyber Issues, and the Working Party on Maritime Issues were invited to take part in a joint thematic session. The Presidency facilitated this inclusive discussion to promote coherence in addressing the physical and cyber aspects of cable resilience.

In April, the Chair of the Horizontal Working Party on Hybrid Threats presented the latest developments regarding the Hybrid Toolbox, supporting integrated implementation of hybrid threat preparedness across domains. The session was also attended by delegates from the Telecommunications Working Party, who contributed to discussions on the draft Council conclusions on reliable and resilient connectivity.

In May, cross-working party coordination continued. The Presidency team of the Horizontal Working Party on Cyber Issues presented the state of play of the negotiations on the Proposal for a Council Recommendation on the EU Blueprint for Cybersecurity Crisis Management, while joint sessions were also held with the Working Party on Maritime Issues (in the context of the EU Maritime Security Strategy), the Telecommunications Working Party, and PROCIV, all invited to contribute to discussions relevant to their respective mandates.

These structured engagements reflected the Presidency's commitment to fostering an integrated approach to resilience, ensuring that policy developments in the CER field are consistent with related efforts in connectivity, cybersecurity, maritime security, civil protection, and hybrid threat response.

At end June, the Presidency plans to invite the Horizontal Working Party on Enhancing Resilience and Countering Hybrid Threats to participate in a joint session, continuing the structured dialogue on integrating hybrid considerations into infrastructure resilience policy.

7. EU-Level Strategic Developments

During the semester, the Polish Presidency gave particular attention to two key EU-level strategic documents with direct relevance for critical entities resilience.

First, the Working Party held a thematic exchange on resilience of critical infrastructure on the report *Safer Together – Strengthening Europe's Civilian and Military Preparedness and Readiness*. The discussion was introduced by the Presidency team of the Ad hoc Working Party on Preparedness, Response Capability and Resilience to Future Crises, which outlined the broader vision of the document. Afterwards, the session allowed Member States to exchange on the most relevant parts of the report regarding critical infrastructure protection. Some delegations noted the importance of enhanced coordination mechanisms between civilian and military actors, shared situational awareness, and scalable crisis response capabilities.

Second, the Commission and the EEAS presented the *Joint Communication on the European Preparedness Union Strategy*, placing specific emphasis on the role of resilient infrastructure as a cornerstone of Union-wide readiness. The exchange that followed gathered different views on how this new strategic framework would support and/or complement the implementation of the CER Directive, particularly in terms of early warning systems, public-private coordination, and the integration of hybrid and climate-related threats into national planning.

8. EU Protective Security Advisors (EU PSA) and Operational Resilience Support

During the March meeting of the PROCIV-CER Working Party, the Commission presented the operational framework of the EU Protective Security Advisors (EU PSA) initiative. The programme is designed to support Member States in strengthening the physical resilience of critical infrastructure through on-site advisory missions, conducted by qualified experts under the coordination of the Commission.

To illustrate the practical value of this tool, a company from the energy sector shared its experience following an EU PSA mission conducted at one of its facilities. The presentation highlighted concrete improvements implemented in response to the advisors' recommendations. The experience was presented as a valuable example of how structured, expert-led engagement can directly enhance resilience at the operator level.

The Presidency underlined the strategic importance of such field-level support mechanisms. In its view, the EU PSA initiative represents a key instrument for enhancing the practical resilience of critical entities and addressing hybrid threats in a targeted, operationally meaningful manner.

9. Integrating Research and Innovation into Resilience Policy

Recognising the importance of research and innovation in strengthening infrastructure resilience, the Presidency will also give visibility to key EU/NATO funded research projects that address different dimensions of critical entity protection. These initiatives exemplify how targeted investment can support practical solutions to evolving risks.

At an upcoming session at end of June, three projects will be presented for the benefit of Member States:

- **R-GRID** - focuses on the use of AI-based threat prediction algorithms to enhance the resilience of power grids;
- **VIGIMARE** - offers a toolbox for subsea infrastructure protection, addressing vulnerabilities in the maritime domain;
- **SARIL** - explores the resilience of European logistics networks, highlighting their function as critical infrastructure and proposing operational models for enhanced robustness.

The Presidency considers it essential to keep Member States informed of relevant innovation efforts and encourages greater synergy between policy implementation and research-based capability development.